SECTION 3
ENVIRONMENT

3.1 EQUIPMENT ENVIRONMENT.

3.1.1 DSRS Server. The DSRS Server will require the following equipment configuration:

a. Sun 4 architecture

b. 500 MB minimum available disk storage

c. Tape Backup Device (available within network)

d. CD - ROM

e. Ethernet connection to the DDN/Internet

f. Modems (based on the number of users dialing in)

g. 16 MB of memory (minimum).

The system configuration listed above should be considered the minimum configuration. The actual CPU size, disk storage, and memory requirements will vary according to the number of users, number and size of the RAs, and RA information in the system. The disk storage specified includes: DSRS executables, configuration files, utility files, unit and system test files, and source files. This disk storage may be computed by multiplying the expected number of RAs by the average size of an RA.

3.1.2 DSRS Client for MS-Windows. The DSRS User for Windows and the DSRS Librarian for Windows will require the following equipment configuration:

a. 486/Pentium IBM PC Compatible 33 MHz (or higher), 486/Pentium IBM PC compatible 50 MHz (or higher) for the Librarian Tool

b. 8 MB memory (minimum)

c. 5 MB available hard disk space (minimum)

d. 3 1/2" 1.44 MB Floppy Disk Drive

e. Ethernet interface adapter or 9600 Baud MODEM (or higher) for PPP/SLIP

f. CD - ROM Drive (optional)

g. Sound adapter with speakers (optional).

3.1.3 DSRS Client for UNIX. The DSRS client for UNIX will require the following equipment configuration:

a. Sun 4 architecture

b. 10 MB minimum available disk storage

c. 16 MB memory (minimum).

3.2 SUPPORT SOFTWARE ENVIRONMENT.

3.2.1 SunOS 4.1.3 Environment.

3.2.1.1 DSRS Server. Support software for the DSRS Server running on the Sun system is shown in Table 3-I.

Table 3-I. Support Software for the DSRS Server

Software	Runtime Environment	Development Environment
SunOS Version 4.1.3 (Solaris 1.1)	●	●
ORACLE7 Server Release 7.1.3.0.0	●	●
ORACLE SQL*Plus Release 3.1.3.4.1	●	●
ORACLE SQL*Net for TCP/IP Version 1.0	●	●
ORACLE PL/SQL Release 2.1.3.0.0.0	●	●
GNU ANSI C Compiler 2.3.3		●
ORACLE Pro*C Release 1.6.4.0.0		●
freeWAIS-0.5	●	●

3.2.1.2 DSRS for X/Motif. The support software for the DSRS X/Motif is shown in Table 3-II.

Table 3-II. Support Software for the DSRS for X/Motif

Software	Runtime Environment	Development Environment
SunOS Version 4.1.3 (Solaris 1.1)	●	●
Open Windows Version 3.0	●	●
ICS OSF Motif Version 1.2.4	●	
ICS OSF Motif Version 1.2.2		●
Minerva MSQL RDBMS Version 1.0	●	
XVT DSC++ Version 3.2		●
SPARCworks Professional C++, SPARCworks 3.0.1		●
SPARCompiler C++ 4.0.1		●
GNU ANSI C Compiler 2.3.3		●
XVT-Graphical Extensions 2.0		●
freeWAIS-0.5	●	●

3.2.2 Solaris 2.3 Environment.

3.2.2.1 DSRS Server. Support software for the DSRS Server running on the Sun system is shown in Table 3-III.

Table 3-III. Support Software for the DSRS Server

Software	Runtime Environment	Development Environment
SunOS Version 5.3 (Solaris 2.3)	●	●
ORACLE7 Server Release 7.1.3.0.0	●	●
ORACLE SQL*Plus Release 3.1.3.4.1	●	●
ORACLE SQL*Net for TCP/IP Version 1.0	●	●
ORACLE PL/SQL Release 2.1.3.0.0.0	●	●
SPARCworks-Pro-C 3.0.1		●
ORACLE Pro*C Release 1.6.4.0.0		●
freeWAIS-0.5	●	●

3.2.2.2 DSRS for X/Motif. The support software for the DSRS X/Motif is shown in Table 3-IV.

Table 3-IV. Support Software for the DSRS for X/Motif

Software	Runtime Environment	Development Environment
SunOS Version 5.3 (Solaris 2.3)	●	●
Open Windows Version 3.3	●	●
ICS OSF Motif Version 1.2.2	●	●
Minerva MSQL RDBMS V1.0	●	●
XVT DSC++ Version 3.2		●
SPARCworks Professional C++, SPARCworks 3.0.1		●
SPARCompiler C++ 4.0.1		●
SPARCworks-Pro-C 3.0.1		●
XVT-Graphical Extensions 2.0		●
freeWAIS-0.5	●	●

3.2.3 MS-Windows Environment.

3.2.3.1 DSRS for MS-Windows and Windows NT. The development support software for the DSRS for Microsoft Windows and Windows-NT is shown in Table 3-V.

Table 3-V. Support Software for the DSRS for Windows and Windows NT

Software	Runtime Environment	Development Environment
Microsoft DOS Version 5.0 (or higher)	●	●
Microsoft Windows Version 3.1/or Windows NT	●	●
Trumpet Winsock 2.1 or Equivalent	●	●
Microsoft Visual Basic Version 3.0		●
Microsoft Access Version 1.1		●
Desaware CCF - Cursors Version 2.0		●
Desaware Custom Control Factory Version 2.0		●
NetManage CHAMELEON Version 3.11		●
Blue Sky RoboHelp Version 3.0		●

The DSRS User Tool that runs on both MS Windows and Windows NT is developed using the support software in Table 3-V.

3.2.3.2 DSRS Librarian for MS-Windows and Windows NT. The support software for the DSRS Librarian for Microsoft Windows and Windows NT is shown in Table 3-VI.

Table 3-VI. Support Software for the DSRS Librarian for Windows

Software	Runtime Environment	Development Environment
Microsoft DOS Version 5.0 (or higher)	●	●
Microsoft Windows Version 3.1/or Windows NT	●	●
ORACLE SQL*Net TCP/IP Version 1.1 for Windows	●	●
Trumpet Winsock 2.1 or Equivalent	●	●
Microsoft Visual Basic Version 3.0		●
Desaware CCF - Cursors Version 2.0		●
Desaware Custom Control Factory Version 2.0		●
NetManage CHAMELEON Version 3.11		●
Borland ReportSmith Version 2.5		●
Blue Sky RoboHelp Version 3.0		●

3.3 COMMUNICATIONS REQUIREMENTS. The communications path between remote sites will take place over the Defense Data Network (DDN)/Internet for the UNIX system. Communications over DDN will be supported via TCP/IP Sockets. Dial-in users will require terminal emulation communications software that supports Serial List Internet Port (SLIP) or Point-to-Point Protocol (PPP). The medium for dial-up terminals is a modem with voice-grade telephone lines.

3.3.1 Graphic Overview. The hardware and software environment will conform to the above listed minimum requirements. A graphical overview of the DSRS communications paths is displayed in Figure 3-1.

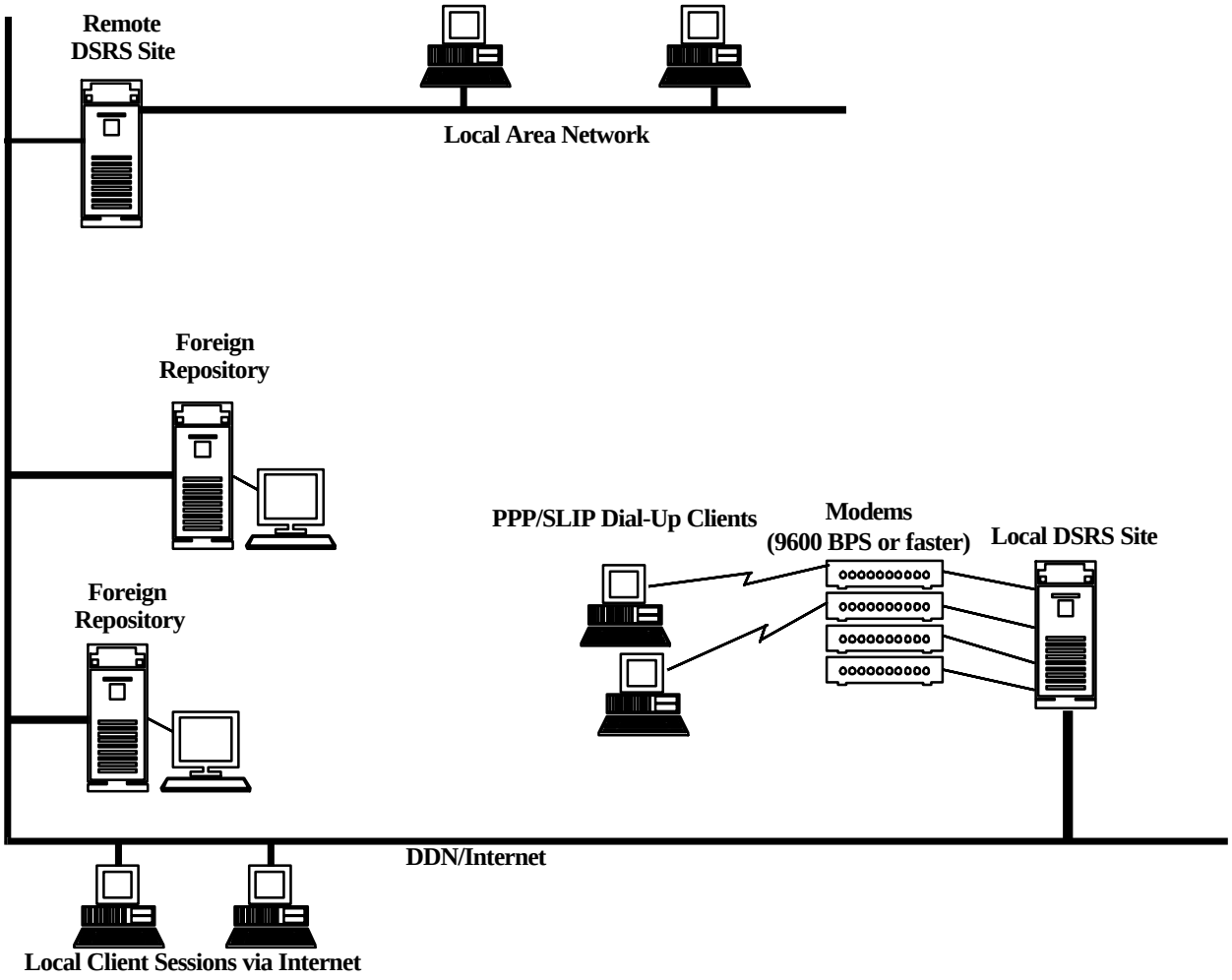

Figure 3-1. DSRS Communications Overview

3.3.2 Hardware. DSRS site computers require appropriate Internet connections to be able to perform remote extractions. This may include Ethernet hardware, routers, and appropriate assignment of Internet addresses.

3.3.3 Software. Software operating on hardware systems described in Section 5.1 will conform to the requirements identified in the previous sections. Users may use various TCP/IP software packages to access the DSRS. Network connections to the Internet will require appropriate Transmission Control Protocol/Internet Protocol (TCP/IP) networking software.

3.3.4 Modems. A modem may be used from a PC to connect to the MS-Windows User Tool. Using a modem to connect to the DSRS requires hardware and software to be installed on the calling end and on the server which is the receiving end. The user needs a recommended minimum 9600 bps modem installed on the calling PC. The TCP/IP software on the user's PC needs a PPP/SLIP option.

The server needs a recommended minimum 9600 BPX modem for users to establish a PPP/SLIP connection with a modem. The TCP/IP software on the server needs a PPP/SLIP option.

Using the modem to connect to the server allows the PC access to the DSRS and the Internet. Access to the Internet is required for proper operation of the DSRS. The PPP/SLIP connection to the server creates the TCP/IP stack necessary for Internet communication.

3.4 INTERFACES. The communication architecture is illustrated in Figure 3-1.

3.4.1 TCP/IP Asset Transfer Interface. The DSRS component transfer is an interaction between two sites (DSRS or foreign) via an application layer protocol transported via TCP/IP. The protocol implements a client/server architecture in which the local DSRS User Tool becomes a client to the Interoperability Server of an owning site. The Interoperability component transfer protocol will provide the basic set of operations for gathering data, transmitting it, and using it properly on the receiving site. This protocol will operate over the Internet and/or local TCP/IP networks. Remote extraction is automated by the DSRS User Tool through the use of the extract command. A user's extract request for remote RAs generates a client transaction to the cooperating site's server; the local DSRS User Tool will communicate with the cooperating site's server. The Interoperability Server located at the remote site will process extract requests and transmit components and extract status to the client.

3.4.2 DSRS-to-ORACLE Interface. Since DSRS uses ORACLE as its underlying database, a communications interface exists between them. The DSRS communicates with ORACLE using SQL and the ORACLE database interface. This communication is local to one computer system; i.e., the DSRS and ORACLE will execute on the same platform.

3.4.3 User Terminal Interface. Users will connect with the DSRS using PPP/SLIP dial-up MS-Windows connections, sessions over the Internet, or X sessions over the Internet. The interface between the user's terminal and the DSRS is provided in large part by the underlying operating system and networking software. X sessions may be executed over a TCP/IP network such as the Internet.

3.5 SECURITY. Based upon the perceived threats, risks, and goals of the DISA Software Reuse Program, the security policy for the DSRS is to provide controlled access protection (C2 functionality). Detailed information concerning security requirements for controlled access protection are included in Appendix A and are derived from the following three basic objectives:

a. Protection and control over who can login to the system.

b. Mechanisms that will enable the DSRS to make decisions regarding access to resources based upon the expressed wishes of its users (with no assurance that concerted, malicious actions cannot circumvent these mechanisms).

c. The capability of generating a reliable log of user actions and to guarantee its correctness.

3.5.1 Logon Protection and Control. Protection and control over who can login to the DSRS is accomplished through a combination of procedural and automated security means. The first step a potential user of the DSRS must accomplish is the completion of an Account Request Form (ARF) that contains a User Non-Disclosure Agreement and a section to be completed by a Government Program Manager/Representative. Both the user and the manager/representative are required to sign the form before an account on the DSRS will be assigned to the user.

Identification and authentication is assured in the DSRS by prompting the user to supply a login name and password. Identification is implemented by asking for a login name which is associated with the user's identity. The DSRS checks this name against its list of authorized users. The system then asks the user to provide a password to authenticate that the user is who he or she claims to be.

3.5.2 Discretionary Access Control. Discretionary Access Control (DAC) is a means of restricting access to named objects based upon the identity of subjects and/or groups to which they belong. DAC is accomplished in the DSRS by assignment of group identifiers to site IDs, user IDs and RA IDs. A group ID is a tag identifying an abstract collection of sites, users, and assets and conveying certain rights and privileges to the members of that collection. Another mechanism in place to control user access in the DSRS is the assignment of specific user types, according to the functions a user will need to perform in the system. The following DSRS user types will be assigned to determine the level of access granted to the user:

a. **Non-User** A person who is identified in the system as being a point-of-contact for an RA. A non-user will not be able to execute the system.

b. **Programmer** A person who will be able to execute the User Tool to identify RAs.

c. **Librarian** A person who maintains the RA Catalog. This user will be able to execute all of the tools associated with the system.

d. **Supervisor** A person who maintains the system catalog. This user will be able to execute all of the tools associated with the system. In addition to Librarian privileges, this user will be able to: delete RAs, add and delete domains, modify local site information, and maintain user accounts for the system supervisors.

3.5.3 Audit. The audit requirements mandate that the system have the capability to create, maintain, and protect, from modification or unauthorized access or destruction, an audit train of accesses to the objects it protects. The DSRS was designed to allow authorized operations and security personnel to generate a number of reports concerning the interactions between subjects (users) and objects (data) in the system. Following is the list of reports supported by the DSRS:

a. pc_server.log

b. lib_server.log

c. dsrs_server.log
d. Usage Log

While not all of the above listed reports were specifically designed with security in mind, the DSRS Security Administrator is able to obtain a complete view of activities on the DSRS system. These logs permit DSRS system audits. Specific details for examination and maintenance of audit reports will be provided in the *DSRS Security Plan* and the *DSRS Trusted Facility Manual*.

Oracle audit capabilities are implemented for the following commands: delete, insert, update, grant all sessions. Information about auditing database usage can be found in the *ORACLE7 Server Administrator's Guide*.